User’s Manual

10/100M Management Switch

Model No.: SP1658B

http://www.micronet.info

Table of Content

1. INTRODUCTION 2

1.1 PACKAGE CONTENT 2
1.2 KEY FEATURES 2
1.3 PHYSICAL DESCRIPTION 3

2. INSTALLATION 4

2.1 INSTALLATION WITHOUT THE RACK 4
2.2 RACK-MOUNT INSTALLATION 4
2.3 INSTALLING NETWORK CABLES 4

3. WEB-BASED USER INTERFACE 6

3.1 SETTING UP CONNECTION 6
3.2 THE HOME PAGE 6
3.3 DEVICE 8
3.4 VERSION INFO 8
3.5 PORTS 9
3.6 SECURITY 11
3.7 SNMP 11
3.8 VLAN 13
3.9 IGMP SNOOPING 16
3.10 PORT AGGREGATION 16
3.11 STA 17
3.12 PRIORITY 21
3.13 ADDRESS TABLE 22
3.14 MIRROR 23
3.15 SNTP 24
3.16 SYSTEM LOG 25

4. TEXT-BASED USER INTERFACE 26

4.1 SETUP THE CONNECTION 26
4.2 MAIN MENU 27
4.3 SYSTEM INFORMATION 27
4.4 MANAGEMENT SETUP 28
4.5 DEVICE CONTROL 28
4.6 USER AUTHENTICATION 30
4.7 SYSTEM UTILITY 30
4.8 SAVE RUNTIME CONFIGURATION 31

5. SPECIFICATION 32

1. Introduction

Micronet SP1658B is a Layer 2 Management Switch that is designed to economically meet the enterprise's needs. With 24 10/100M ports and 2 Gigabit ports, it provides non-blocking transmission and allows choosing either copper or mini-GBIC slots for Gigabit expansion without any proprietary modules. Moreover, it brings advanced features, as tag-based VLAN, port aggregation, Class of Service (802.1p), and bandwidth control. All of these features are configurable via various management interfaces, including RS-232 console, TELNET, HTTP, and SNMP.

1.1 Package Content

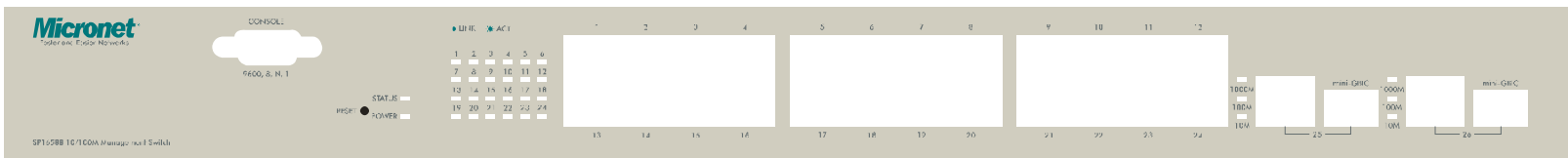
Before you start installing the device, verify the following items are in the package:

- SP1658B Management Switch
- Quick Installation Guide
- Manual CD
- Power cord
- RS-232 cable
- Rack-mount brackets
- Rubber foot and screws

1.2 Key Features

- Compliant with IEEE802.3 10Base-T, IEEE802.3u 100Base-TX, IEEE802.3ab 1000Base-T, IEEE802.3z 1000Base-LX/SX, IEEE802.1q tag-based VLAN, and IEEE802.1p traffic classification (CoS) standards
- Support auto-link and auto-negotiation for all RJ-45 ports
- Provide 2 mini-GBIC slots for fiber extension
- Support Port Aggregation and up to 7 groups
- Support port-based VLAN up to 26 groups
- Support 802.1Q VLAN and up to 255 groups
- Support spanning tree protocol: IEEE802.1d STP
- Support IGMP snooping
- Support 2 priority queues per port and CoS policies: Weighted Round Robin (WRR)
- Support bandwidth control per port
- Support IP lock to control access to the switch
- Support SNMPv1 for network management
- Support MIBs: MIB II, Bridge MIB, private enterprise MIB
- Support web-based and menu command (telnet, console) configuration interfaces
- Support 8MB SDRAM for run time data storage
- Support 2MB Flash EPROM for cooperation and configuration data storage
- Support 6K MAC address entries
- Support 384KBytes packet buffer

1.3 Physical Description



SP1658B front view

RESET Button

The button provides users to restart the switch.

LED Status

Please refer to the following table for LED definition

LED	Status	Operation
POWER	On/Green	Power is on
	Off	Power is off
Status	On/Green	System OK
	Off	System fails

10/100M Ports:

LINK/ACT	On/Green	Link detected
	Blink/Green	Traffic detected
	Off	No link

Gigabit Ports:

1000M	On/Green	1000M link detected
100M	On/Green	100M link detected
10M	On/Green	10M link detected

Note: The two RJ-45 ports #25 & #26 are respectively shared with the two mini-GBIC slots.

2. Installation

This switch can be placed directly on your desktop, or mounted in a rack. If you install the device in a normal-standalone standard, the switch is an Intelligent Switch, and users can immediately use most of the features simply by attaching the cables and turning the power on.

Before installing the switch, we strongly recommend:

1. The switch is placed with appropriate ventilation environment. A minimum 25mm space around the unit is recommended.
2. The switch and the relevant components are away from sources of electrical noise such as radios, transmitters and broadband amplifiers
3. The switch is away from environment beyond recommend moisture

2.1 Installation without the Rack

Install the switch on a level surface that can support the weight of the unit and the relevant components. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet. Attach the provided robber feet to the bottom of the switch to keep the switch from slipping. The recommend position has been square-marked.

2.2 Rack-mount Installation

The switch may standalone, or may be mounted in a standard 19-inch equipment rack. Rack mounting facilitate to an orderly installation when series of networking devices circumstance needed. The switch is supplied with rack mounting brackets and screws for rack mounting the unit.

Procedures to Rack-Mounting the Switch in the 19-inch rack:

1. Disconnect all cables from the switch before continuing.
2. Place the unit the right way up on a hard, flat surface with the front facing you.
3. Locate a mounting bracket over the mounting holes on one side of the unit.
4. Insert the screws and fully tighten with a suitable screwdriver.
5. Repeat the two previous steps for the other side of the unit.
6. Insert the unit into the 19" rack and secure with suitable screws (not provided).
7. Reconnect all cables.

2.3 Installing Network Cables

Station Connections

Connect each station with proper cables. For correct cable type, please refer to “Wiring for the 24+2G Mini GBIC SNMP Switch” in section 2.3.

Switch-to-Switch Connections

In making a switch-to-switch connection, use Gigabit ports to connect another switch or backbone is strongly

recommended. The Gigabit ports provide the fat pipe to the server or backbone for boosting the total system performance. Please refer to “Wiring for the 24+2G Mini GBIC SNMP Switch” in section 2.3 and connect the switch with correct cable types.

Note: The switch supports port aggregation (port trunk) can further enhance the transmission speed in switch-to-switch connectivity. The port trunk function supports up to 7 aggregation groups, which consist of 4 ports per group to create bandwidth up to 800Mbps.

3. Web-based User Interface

3.1 Setting up Connection

This switch can be managed using a standard Web Browser from any computer attached to the network. The SNMP management feature also permits the switch to be managed from any SNMP network management station running a network management program. Factory Default value of system is:

IP Address:	10.10.0.1
Subnet Mask:	255.255.0.0
Default Gateway:	10.10.0.254

This Web Browser User Interface is coded by Java Applet and running on the JavaTM Virtual Machine (JVM) version 1.3.1 platform. You should configure the management station with an IP address and subnet mask compatible to your switch for accessing. Also, the management station should be well configured and connected to Internet for automatically downloading (upgrading) the suitable JVM through Internet from "http://java.sun.com". Or you can download it yourself by the URL "http://java.sun.com/j2se/1.3/download.html" and manually install it. Running your Web Browser and enter the IP address "10.10.0.1" as the URL in the "address" field. After authentication procedure, the home page shows up.

Note: Occasionally the newer JavaTM Virtual Machine is not backward compatible, that JVM version 1.3.1 is strongly recommended to ensure properly operation.

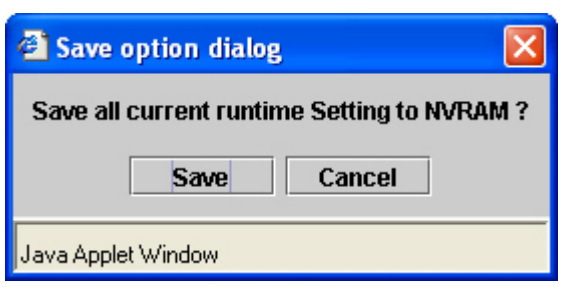
Login account by default is:

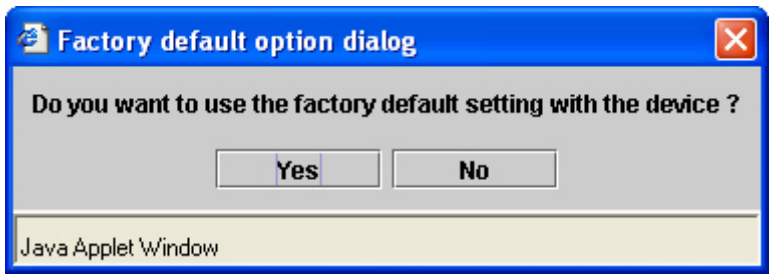
Username: ***admin*** Password: ***admin***

Note: admin can do any configuration except changing password.

3.2 The Home Page

This page shows all available system tools for switch management.

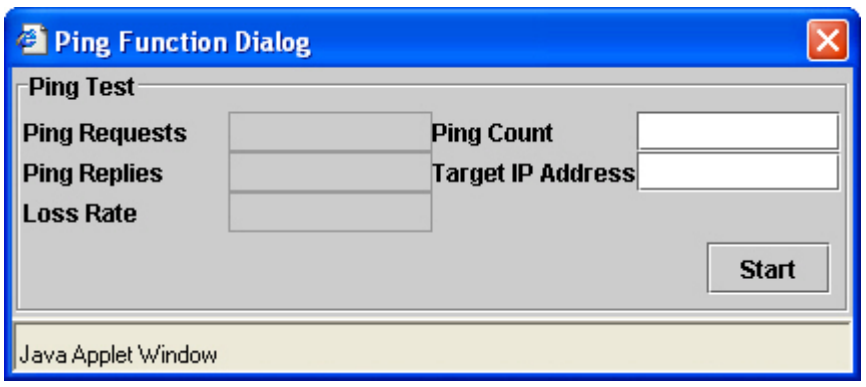
Function	Statement
<Save>	Save the current setting to Non-volatile Memory. The difference between <Save> and <Apply> is that Apply applies settings right away but saves the values in the system memory. By every switch reboot, system obtains system parameters from Non-volatile Memory you <Saved> before but not buffer memory. Click "Save" button to save it to Non-volatile Memory. 
<Default>	To make the switch restore default value. Click "Default" button to apply the switch with initial value. If you want to clear the previous value in the Non-volatile Memory, please <Save> it.



<Reboot> Warm Boot: Boot the switch without Power On Self Test (POST) to shorten the booting time.

Cold Boot: Boot the switch and with fully Power On Self Test.

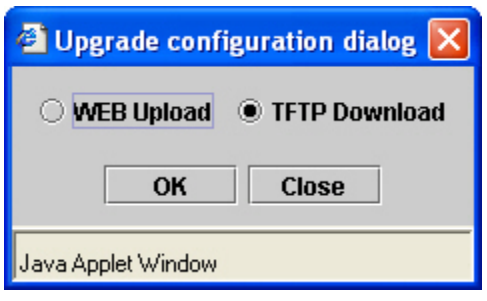
<Ping> To Ping is a commonly used tool to detect existence of the remote host or IP address. Also, the network status can be known by the ratio of packets Reply and Loss.



<Telnet> To begin the Telnet program. The login screen pops up by simply clicking the <Telnet> button.

<Contact> Contact technicians for technical support by E-Mail

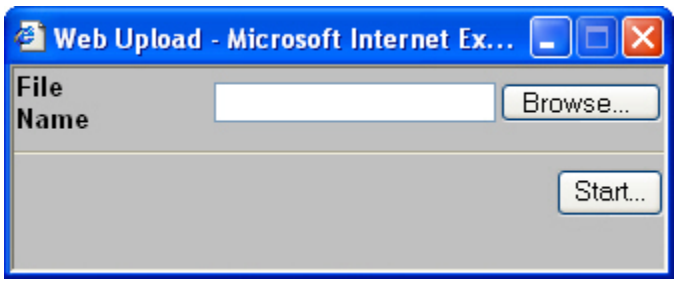
<Upgrade>



WEB Upload

Select Device ID and “WEB Upload” radio button then click OK

Specify the file path by clicking Browse button and click Start to trigger.



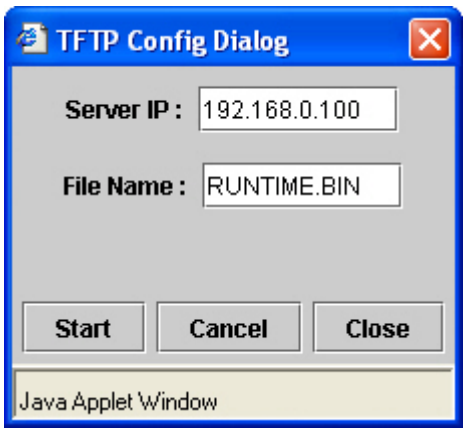
TFTP Download

Select Device ID and “TFTP Download” radio button then click OK

Enter the TFTP server’s IP address in Server IP field

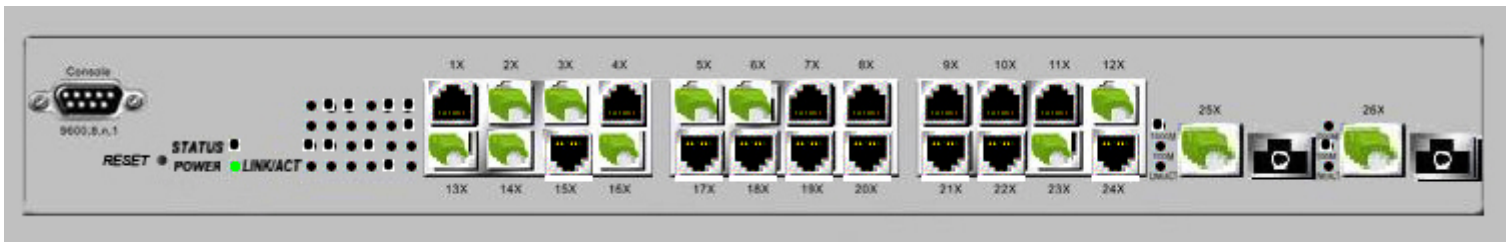
Enter file name in File Name field

Click Start button to download the code for system to update with it automatically.



3.3 Device

Panel Display



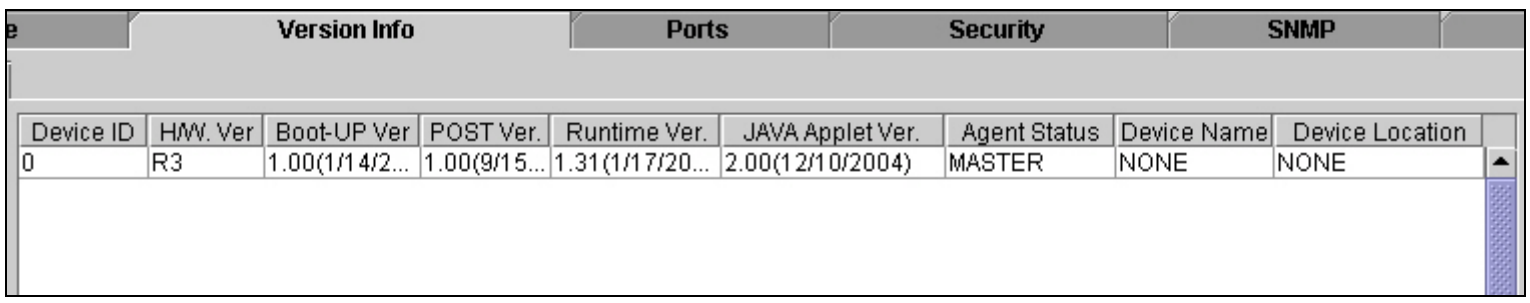
Network Configuration

IP Address	IP address of this device
Subnet Mask	NetMask of your network
Gateway IP	IP address of Gateway

Device Information

Name	Naming the system (optional)
Contact	Who the System administrator is (optional)
Location	Where the management stack locates (optional)

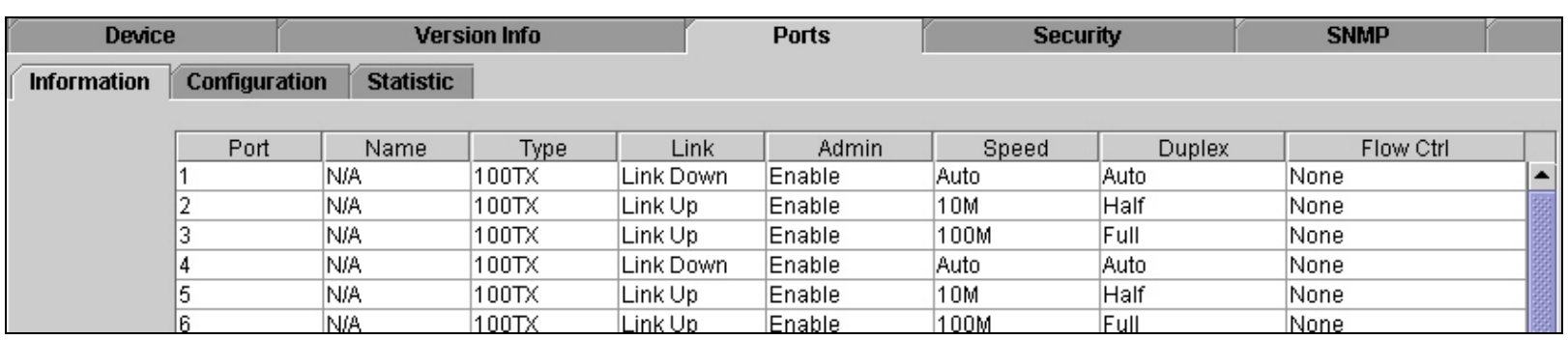
3.4 Version Info



3.5 Ports

Information

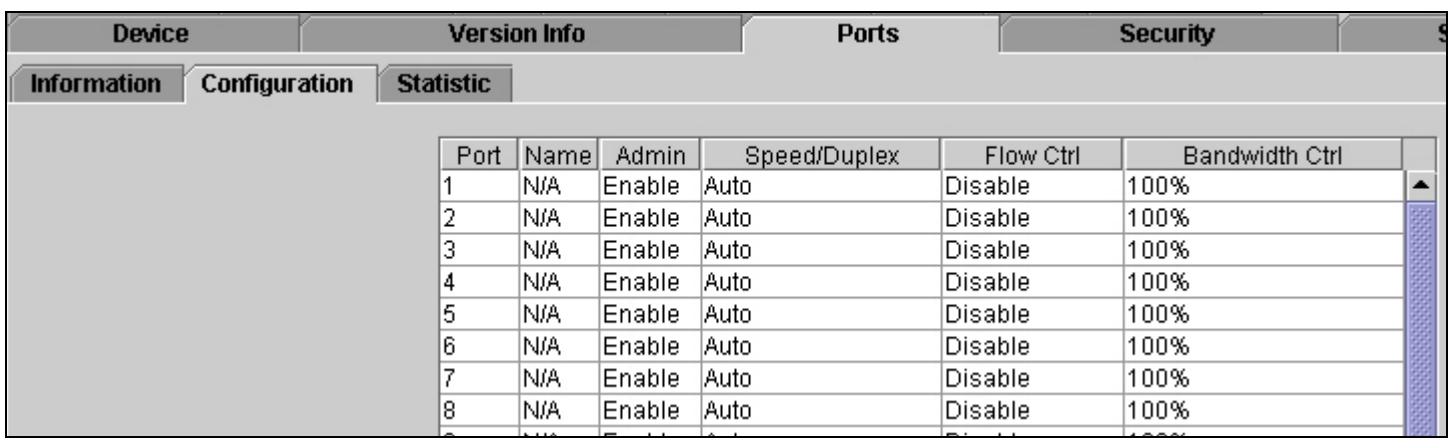
The Information screen shows a summary table of port configuration. You can know the status of each port clear at a glance via information provided including Link Up/Link Down, Enable/Disable, Link Speed, Duplex mode and Flow Control.



(Note: Also by simply clicking the port on the ‘Panel Display’, the port information screen pops up.)

Configuration

Port attributes can be setup in this page.



Name: Enter a name for identification,(ex, ‘Richard’); and press Enter

Admin: Leave the column ‘Enable’ to make the port to be in operation or ’Disable’ to pause it

Speed/Duplex: 10Half, 10Full, 100Half, 100Full, Auto

Flow Control: Select ‘Enable’ to take “Flow Control” effect

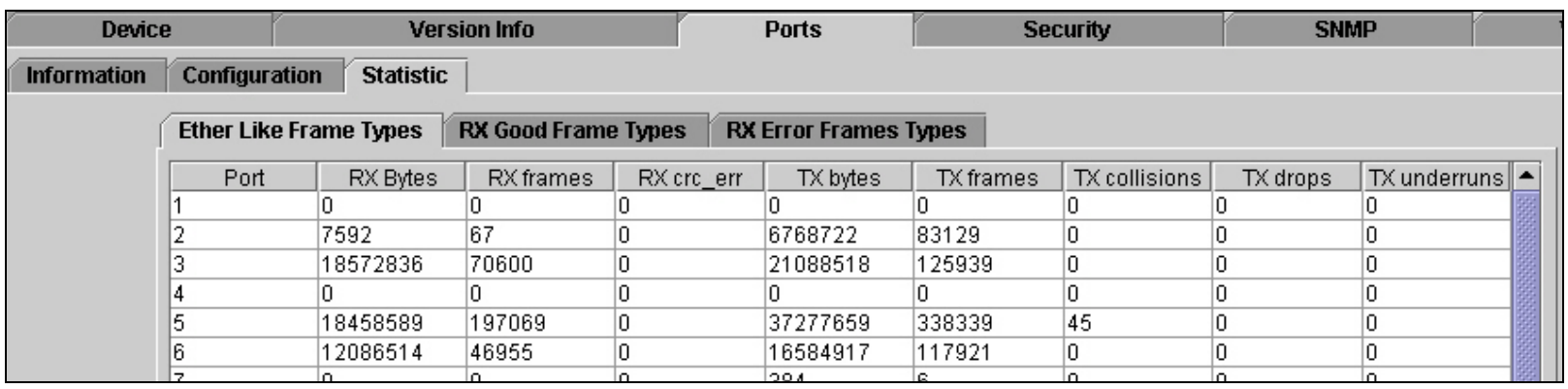
Bandwidth Ctrl: Select the predefined “Bandwidth Control” scale (10%~100%)

Click Apply button to apply settings

Flow Control operation mode:

Speed / Duplex mode	Flow Control
10 Half	Back pressure
100 Half	Back pressure
10 Full	IEEE 802.3x Pause Frame
100 Full	IEEE 802.3x Pause Frame
1000 Full	IEEE 802.3x Pause Frame

Statistic



Port	RX Bytes	RX frames	RX crc_err	TX bytes	TX frames	TX collisions	TX drops	TX underruns
1	0	0	0	0	0	0	0	0
2	7592	67	0	6768722	83129	0	0	0
3	18572836	70600	0	21088518	125939	0	0	0
4	0	0	0	0	0	0	0	0
5	18458589	197069	0	37277659	338339	45	0	0
6	12086514	46955	0	16584917	117921	0	0	0

Ether Like Frame Types

RX Bytes	Number of bytes received in good and bad frames
RX Frames	Number of good and bad packets received
RX crc_err	Number of CRC errors received
TX Byte	Number of bytes transmitted in good and bad frames
TX Frames	Number of good and bad packets transmitted
TX Collisions	Number of collisions on transmitted frames
TX drops	Frames dropped due to lack of receive buffer
TX underruns	Increments when packet transmission fails due to the inability of the interface to retrieve packets from the local packet buffer fast enough to transmit them onto the network

RX Good Frame Types

RX Bytes	Number of bytes received in good and bad frames
RX frames	Number of good and bad packets received
RX broadcasts	Number of good broadcasts
RX multicasts	Number of good multicasts
RX less64_pkts	Number of short frames with invalid CRC (<64 bytes)
RX 65to127_pkts	Number of 65 to 127-bytes frames in good and bad packets
RX 128to255_pkts	Number of 128 to 255-bytes frames in good and bad packets
RX 256to511_pkts	Number of 256 to 511-bytes frames in good and bad packets
RX 512to1023_pkts	Number of 512 to 1023-bytes frames in good and bad packets
RX 1024more_pkts	Number of 1024 to max-length-type frames in good and bad packets

RX Error Frame Types

RX alignment_err	Number of alignment errors received
RX crc_err	Number of CRC errors received
RX oversize_err	Number of long frames with valid CRC
RX undersize_err	Number of short frames with valid CRC
RX fragments_err	Number of short frames with invalid CRC
RX jabbers_err	Number of long frames with invalid CRC

3.6 Security

For security reason, you can specify the Station IP address to prevent other user to access this switch. There are five sets for you to add.

To Add IP:

Enter the IP address in the textbox

Click **<<Add** to add the new IP

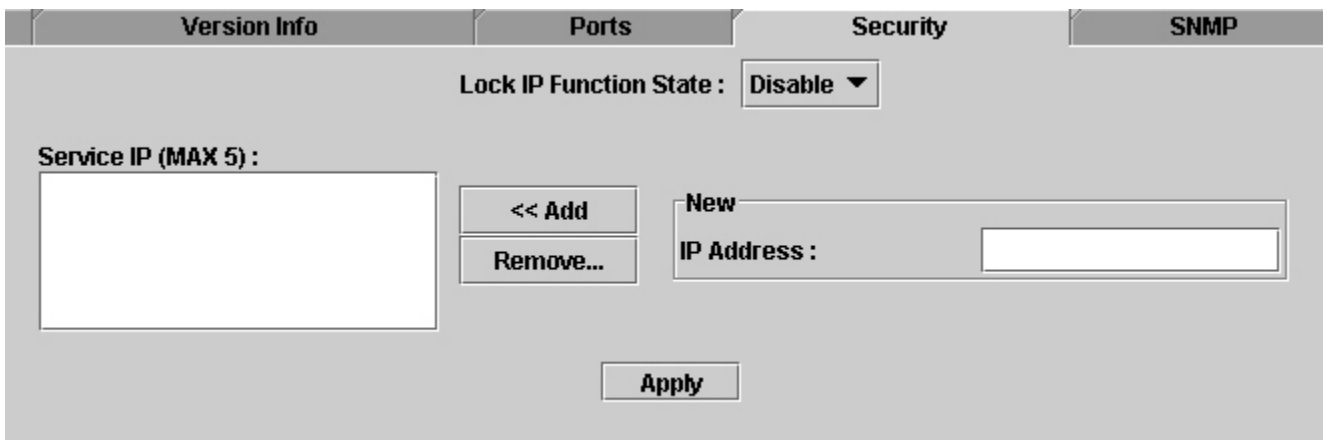
To Remove IP:

Select the Service IP you want to remove

Click **Remove…**

To Enable or Disable:

Select **Enable** or **Disable** in the Lock IP Function state



3.7 SNMP

Simple Network Management Protocol (SNMP) is a communication protocol for managing devices on a network. It is commonly used for network administrators to communicate with multiple devices (hub, switch, router …) for configuring and monitoring while convenient for troubleshooting but no miscellaneous platform consideration.

The built-in SNMP is an agent, which watches the status of it self. The Network Management Station (A computer attached to network with SNMP management program well installed) can be used for accessing to.

Community

A valid entry of Community String and IP Address is for authentication to login to the SNMP agent for configuration. Moreover, the community capacity can up to 3 sets and only by the way of specified IP address here will be allowed to access the agent. One entry consist of IP address “0.0.0.0” will allow the ones who know the community string to access the agent (with Read-Only access right) without limitation.

To Add a community:

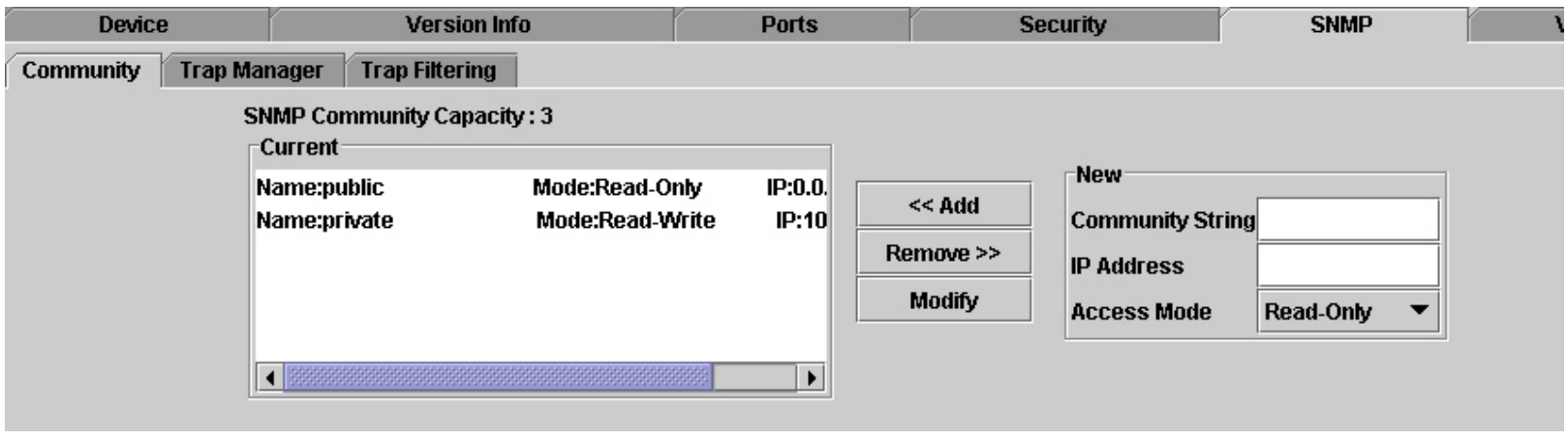
Input a name as a community string for authentication in the “Community String” field (ex: administrator)
Enter the IP address in the “IP address” field you allow to access from (ex: 192.168.1.22).
Click the “Access Mode” combo box and select an authority (Read-Only / Read-Write).
Click **<<Add** button to add this entry.

To Remove a Community:

Select the community you want to remove from the “Current” list.
Click **Remove>>** button to remove it.

To Modify a Community:

Select one community you want to modify in the “Current” column.
The “New” column lists the corresponding values; please modify it.
Click **Modify** button to update the entry.



Trap Manager

Trap Manager specifies the Network Management Stations (NMS) that will receive trap messages from the SNMP agent and can up to 5 entries. A Trap Manager entry with Aging Time “0” will never expire; and Aging Time “10” will expire when 10 minutes is up and no trap messages can corresponding entry receive.

To Add a Trap Manager:

Input a name for authentication in the “Community String” field (ex: administrator).
Enter the IP address in the “IP address” field you allow to access from (ex: 192.168.1.22)
Enter a expiry time for this entry will be durable in minutes (“0” for never expires).
Click **<<Add** button to add the entry.

To Remove a Community:

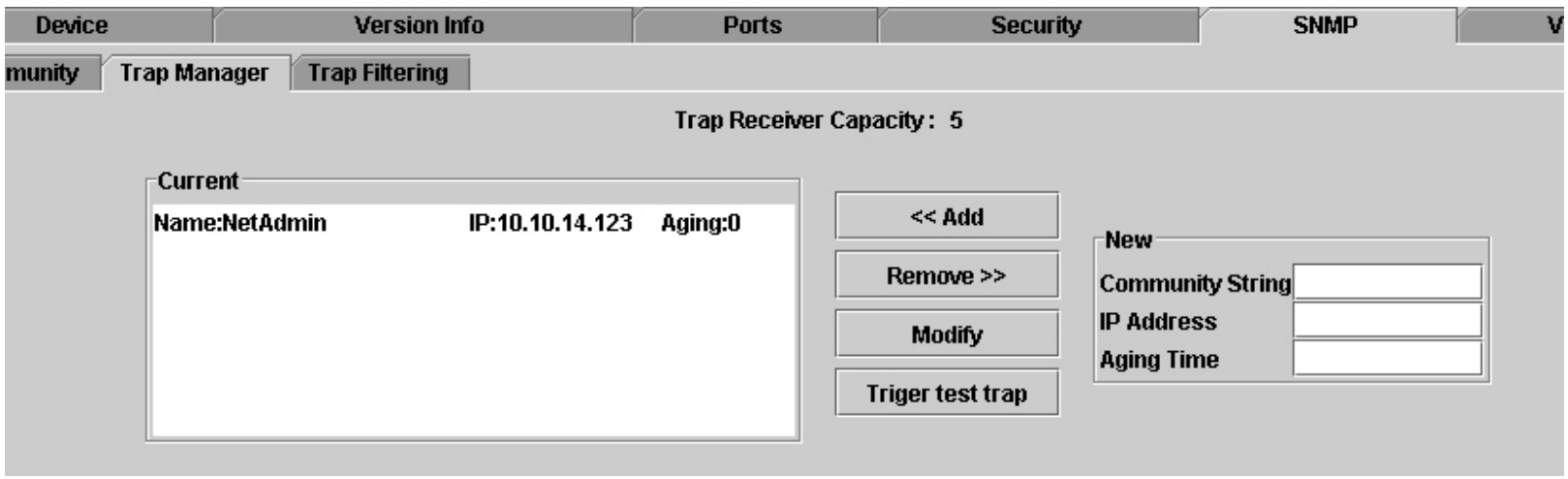
Select the community you want to remove from the “Current” list.
Click **Remove>>** button to remove it.

To Modify a Community:

Select one community you want to modify in the “Current” column.
The “New” column lists the corresponding values; please modify it.
Click **Modify** button to update the entry.

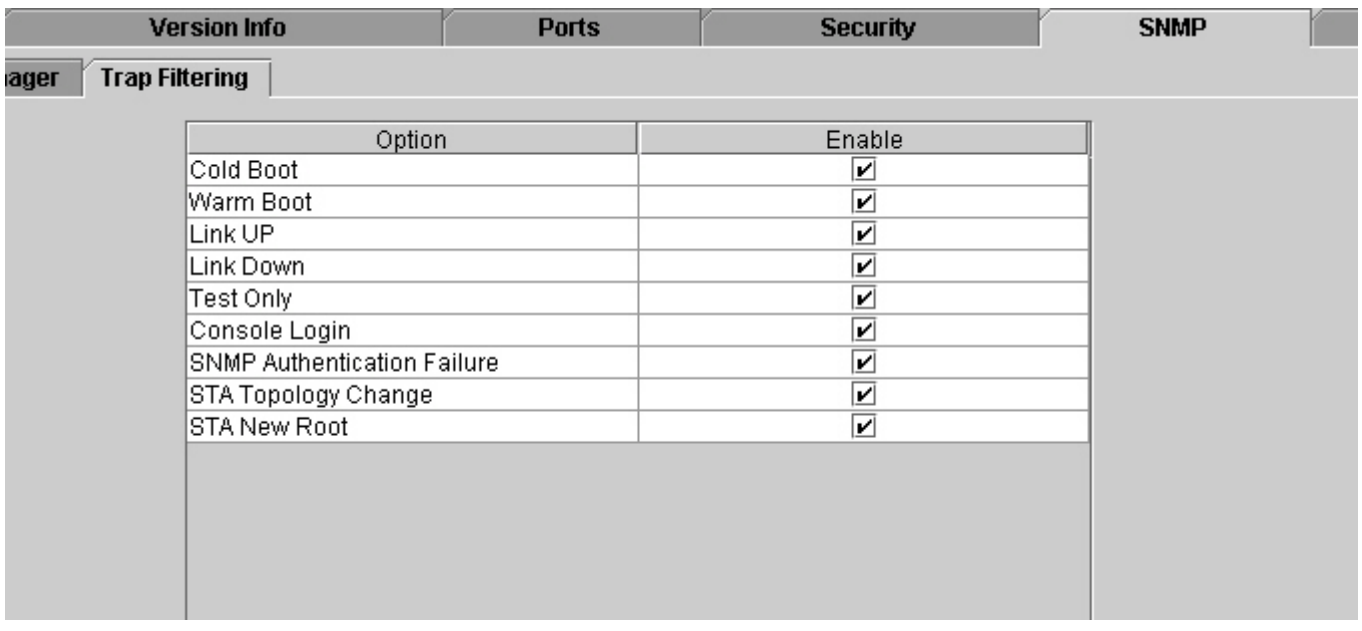
Trap Manager

Press Trigger test trap button, one test trap will be sent to all NMS that have been added to Trap Manager list.



Trap Filtering

Check the “Enable” boxes by mouse clicking to receive a notice when corresponding event occurs. Reserve means reserve for future update.



3.8 VLAN

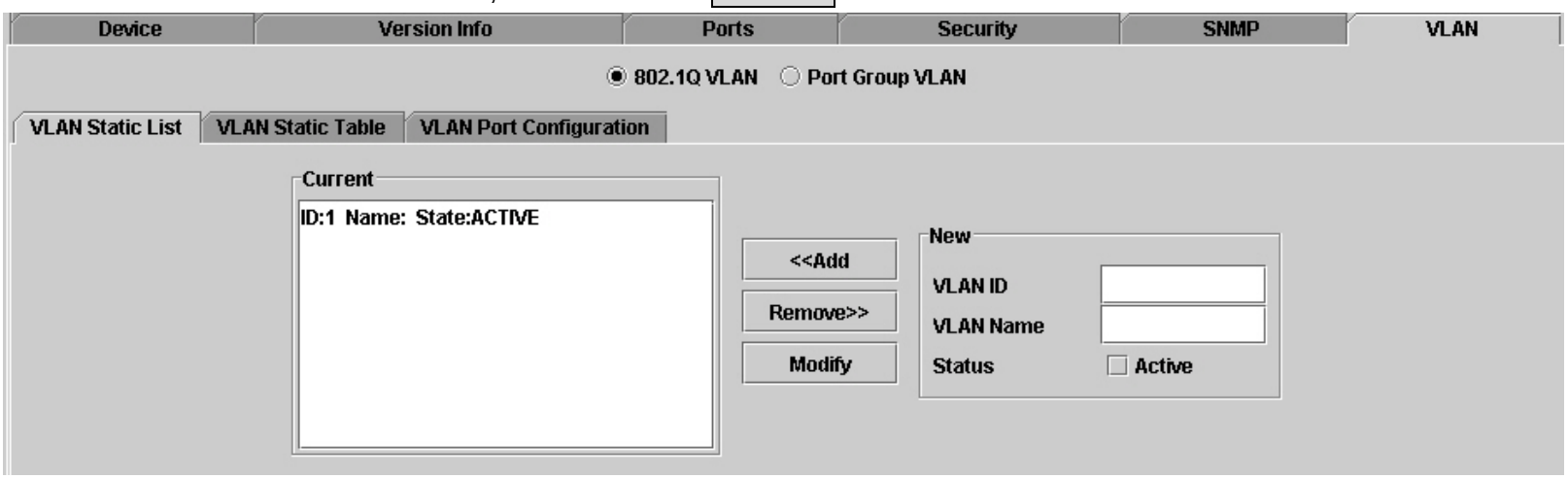
The VLAN functions a group of ports that may spread around the network to communicate as though they belong to one subnet. It doesn’t only provide **Port-based VLAN** to divide whole the network into subnets, but also **802.1Q VLAN** compliant VLAN to recognize all ports into separate broadcast domains for security reasons and reduce collision to obtain efficient bandwidth usage. It produces cleaner network environment by reducing broadcast traffic and simplify network management by allowing moving devices to another VLAN without changing physical connections.

802.1Q VLAN:

VLAN Static List

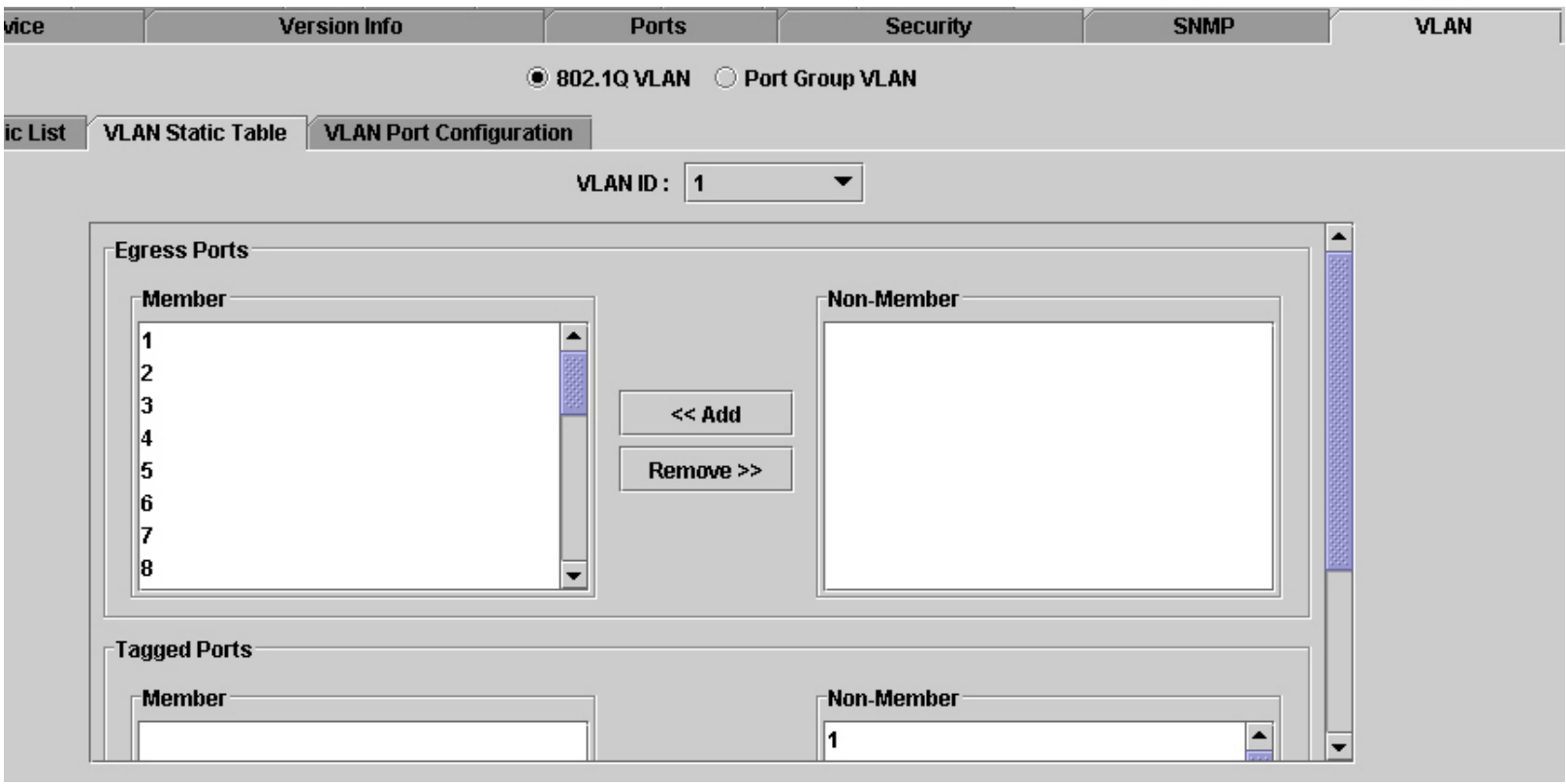
Right here you can add new VLAN groups.

Just enter **VLAN ID** & **VLAN Name**, and then click **<<Add**.



VLAN Static Table

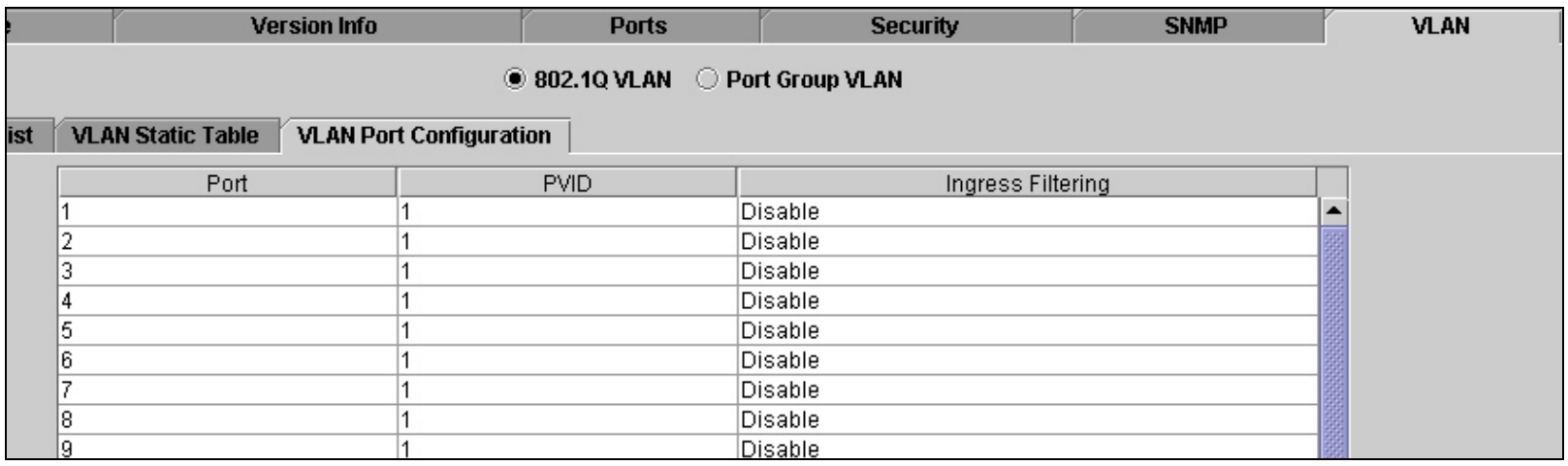
Right here you configure VLAN members for the created VLAN groups. When the switch receives packets, packets will be tagged and forwarded to all ports within the VLAN group.



Note: Packets go out of the tagged port and are still tagged with VLAN ID. However, packets go out of the Egress port and VLAN tag will be removed.

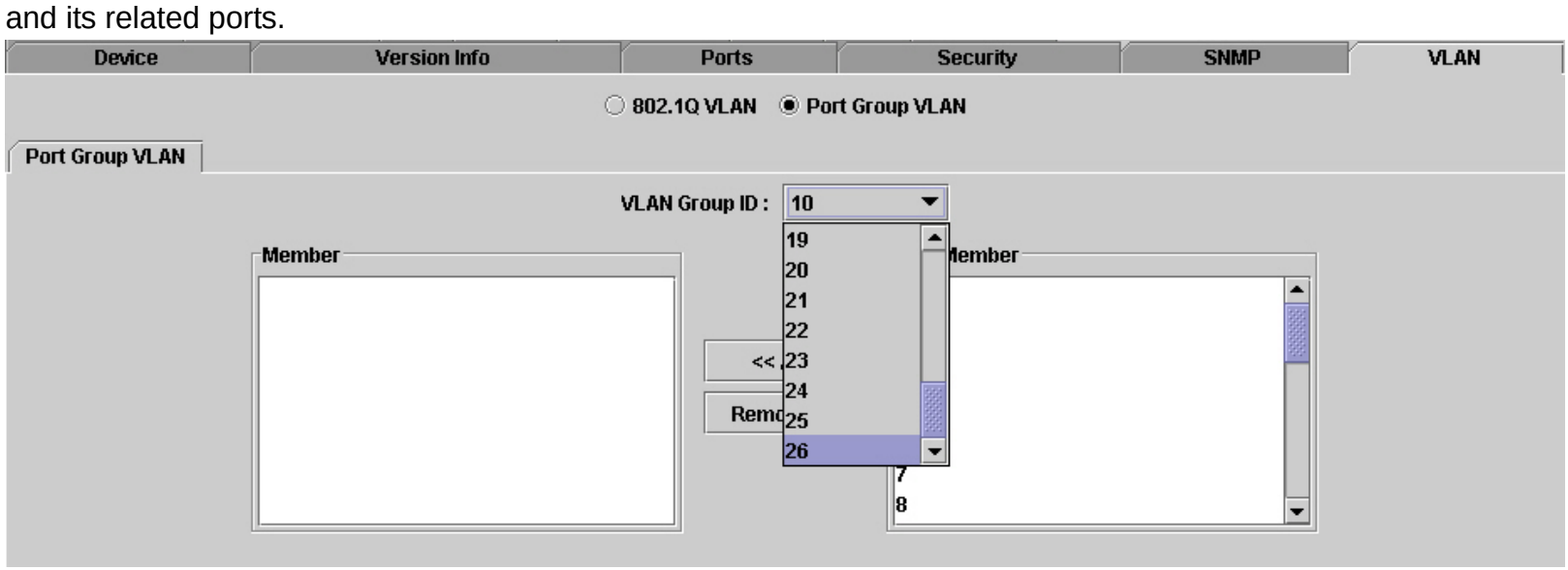
VLAN Port Configuration

Right here you configure PVID (Port VID) for each port. When the switch receives packets on the port, packets will be tagged with VLAN ID according to PVID of the incoming port.



Port Group VLAN:

The Port Group VLAN (Port-based VLAN) is concentrate on definite ports. The packets forwarding policies are based on destination MAC addresses or related ports by voluntary learning relationship of MAC addresses and its related ports.



To add member port:

Click the “VLAN ID” combo box (1 ~ 26) and select a VLAN you want the new ports to join in.

Select ports (press Shift/Ctrl key for selecting multi ports) in the “Non-Member” column.

Click **<<Add** button to join selected ports in.

To remove member port:

Click the “VLAN ID” combo box and select the VLAN you want to remove ports.

Select ports (with Shift/Ctrl key to select multi ports) in the “Member” column.

Click **Remove>>** button to delete selected ports.

All Together:

Click **All Together** button then all the ports of the switch will be added to VLAN group 1.

All Independent:

Click **All Independent** button then all the ports will be divided into separated subnets, that are 26 subnets.

Every port can be belonged to different Port Group VLANs simultaneously without limitation.

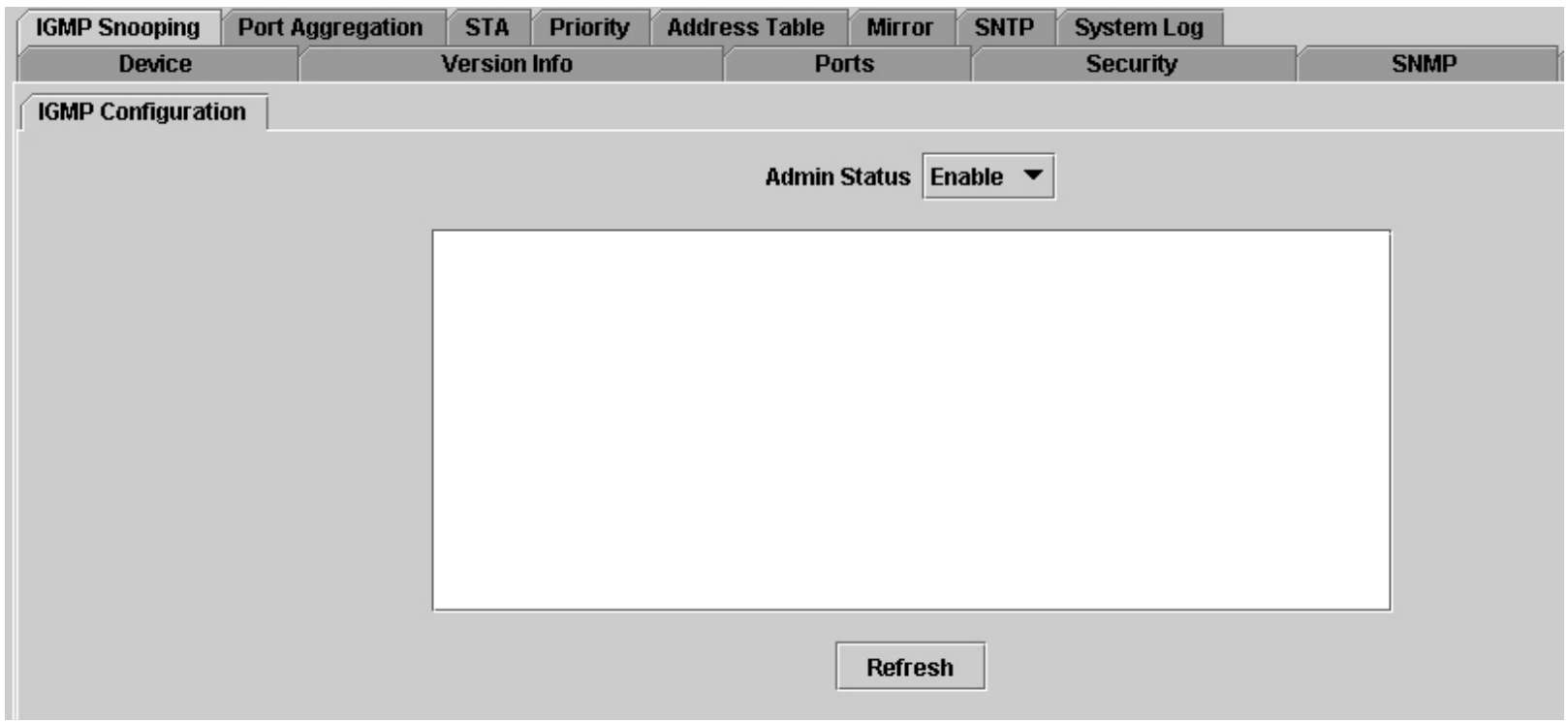
Note: If a removed port is no longer belonging to any other group, it is temporarily disabled because no one can communicate with it. The port which is assigned a PVID and the PVID is equal to VLAN ID, removing the

port will not allow until you change it.

3.9 IGMP Snooping

Multicasting is widely used to support multi-media applications such as video conferencing. The multicasting simply broadcasts its services to the group of a network instead of establishing connections separately with every host that subscribed the services. With no Multicast Filtering-aware switches, a multicast server may floods broadcast-data overall the broadcast domain and wastes a lot of bandwidth.

The Internet Group Management Protocol (IGMP) snooping uses the protocol to make switches join/leave multicast group and interacts switches to optimize the network performance by monitoring the IGMP packets and forward to the ports containing multicast hosts or switches. This will efficiently reduce the multicast traffic rather than flooding overall network. IGMP snooping is more and more important by the booming of multi-media demand.



Note: As IGMP Snooping only operates under 802.1Q VLAN mode, please change VLAN mode from Port Group VLAN to 802.1Q VLAN before enabling IGMP Snooping.

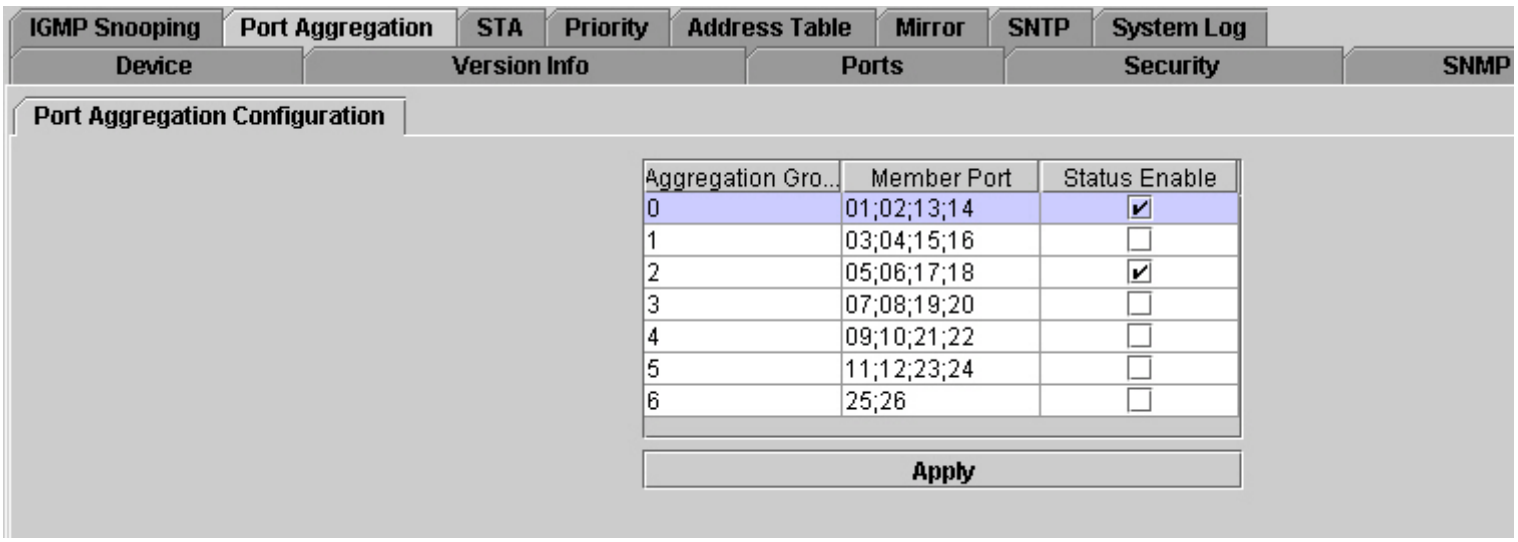
3.10 Port Aggregation

Port Aggregation (Port Trunk) is used to increase the bandwidth of a switch-to-switch connection and backup. This switch provides 7 port aggregation groups, which consist of 4 ports and create bandwidth up to 800Mbps per group at full duplex mode (group 6 consists of the 2 Gigabit ports). Check the box of Aggregation Group in the Status Enable column and press **Apply** then the selected Aggregation Group is activated.

However, before making connections between switches, pay attention to:

- The ports at both ends of a Port Aggregation connection must be configured as Aggregation Ports
- The ports at both ends of a Port Aggregation connection must have the same port properties, including Speed, Duplex mode
- All the ports of a Port Aggregation must be treated as an integer when added to/deleted from a VLAN.

- Spanning Tree Algorithm (STA) treats all the ports of a Port Aggregation as an integer. Before connecting cables between switches, enable the Port Aggregation to avoid looping. Before disabling Port Aggregation, remove the connecting cables between switches to avoid looping.

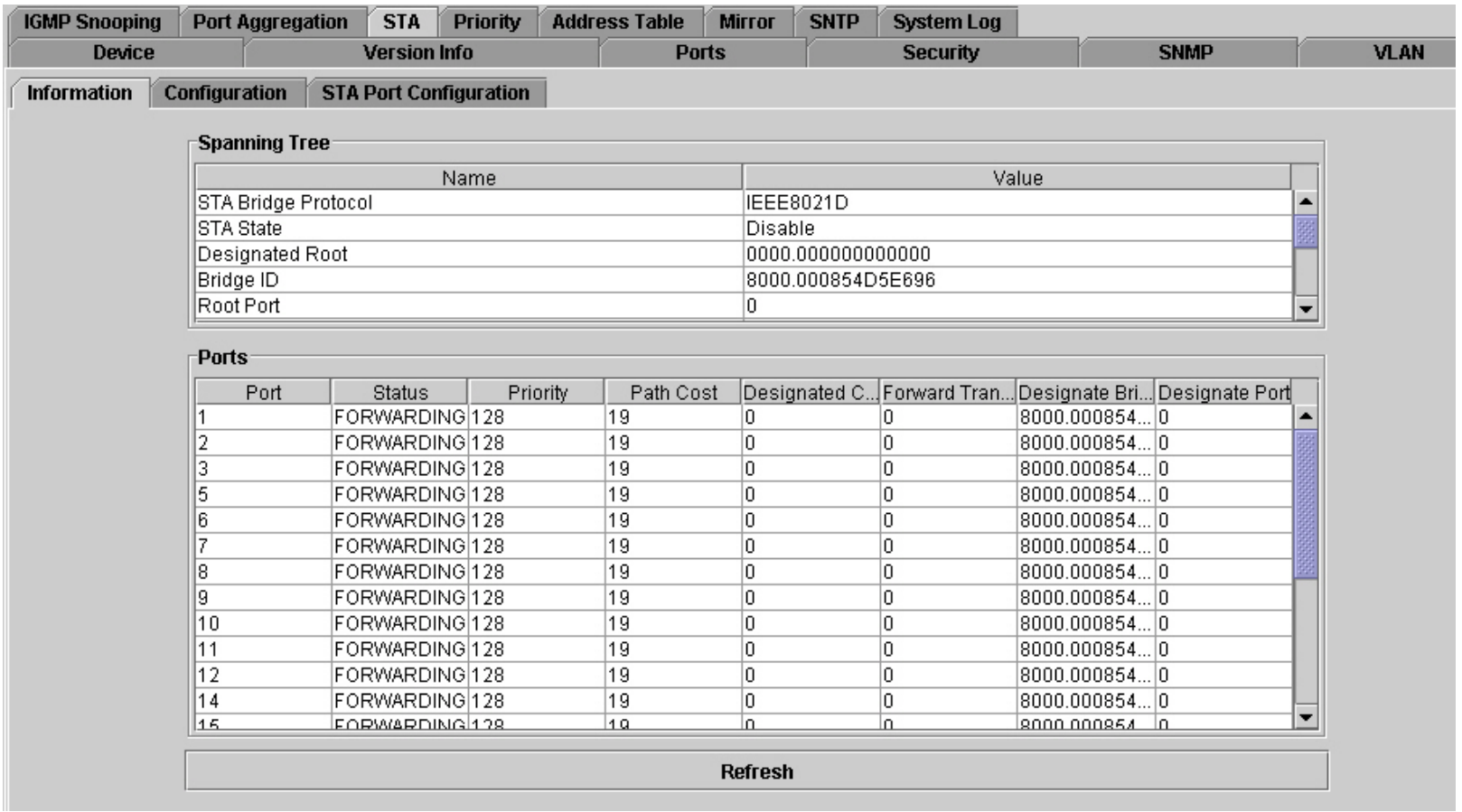


3.11 STA

The Spanning Tree Algorithm (STA) outlined in IEEE 802.1D can avoid network looping but coexist with linking backup. This feature permits STA-aware switches interact with each other. This can ensure only one route exists between any two devices on the network. If looping is detected (maybe implements on purpose for linking backup), looping ports will be blocked to discard additional route. If one using route fails, this Spanning Tree Algorithm automatically releases the blocking port and establishes connection with other devices. Since a STA network has been established, all devices listen for Hello BPDUs (Bridge Protocol Data Units) sent from the Root Bridge. After the Max Age maximum time is up, the device supposes that the route to the Root Bridge is down. The devices initiate negotiations with each other to reconfigure the network for a valid topology.

Information

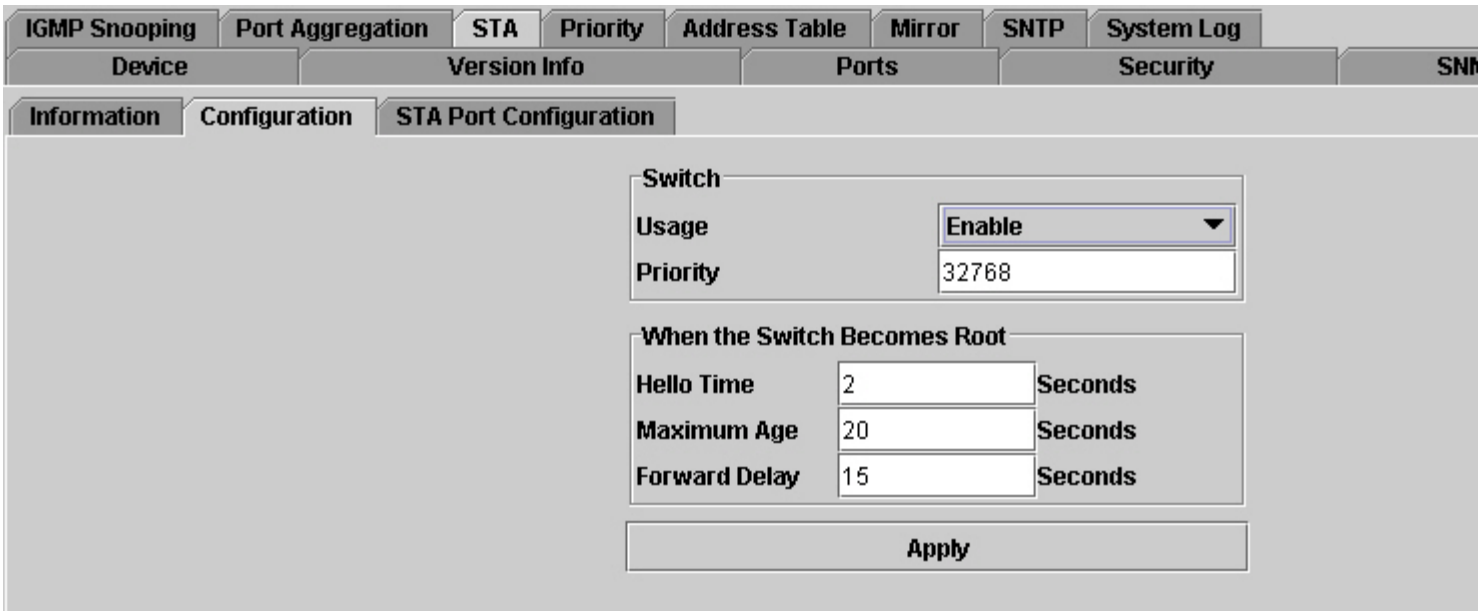
This screen displays summaries of STA information. For further configuration, please go to next session.



Parameter	Description
STA State	Shows if STA is enabled on the switch and participated an STA compliant network
Designated Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached
Bridged ID	The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique
Root Port	The port number of the port which offers the lowest cost path from this bridge to the root bridge
Max Age (6~40 sec)	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of a second. This is the actual value that this bridge is currently using
Hello Time (1~10 sec)	The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so, in units of a second. This is the actual value that this bridge is currently using
Hold Time	This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of a second

Forward Delay (4~30 sec)	This time value, measured in units of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database
Root Path Cost	The cost of the path to the root device as seen from this bridge
Configuration Changes	The total number of topology changes detected by this bridge since the management entity was last reset or initialized
Last Topology Change	The time (in a second) since the last time a topology change was detected by the bridge entity

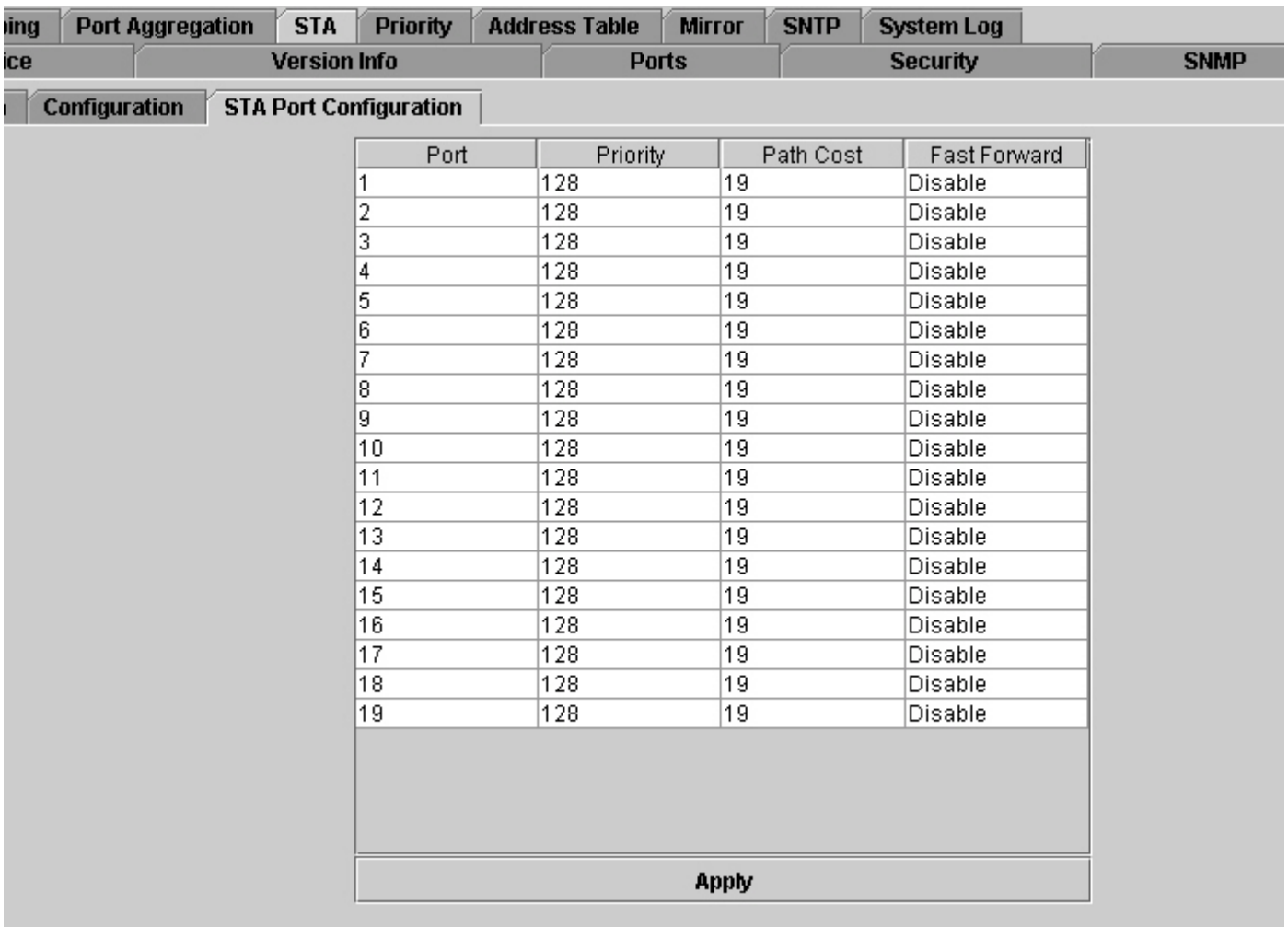
Configuration



Usage	Enable/Disable this switch to join in/withdraw from a STA compliant network
Priority (1~65535)	Priority is a decisive key for selecting root device, root port, and designated port. The smaller number, the higher priority. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device
Hello Time (1~10sec)	The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so, in units of a second. This is the actual value that this bridge is currently using
Maximum Age	The maximum age of Spanning Tree Protocol information learned from

(6~40sec)	the network on any port before it is discarded, in units of a second. This is the actual value that this bridge is currently using
Forward Delay (4~30sec)	This time value, measured in units of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used, when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database

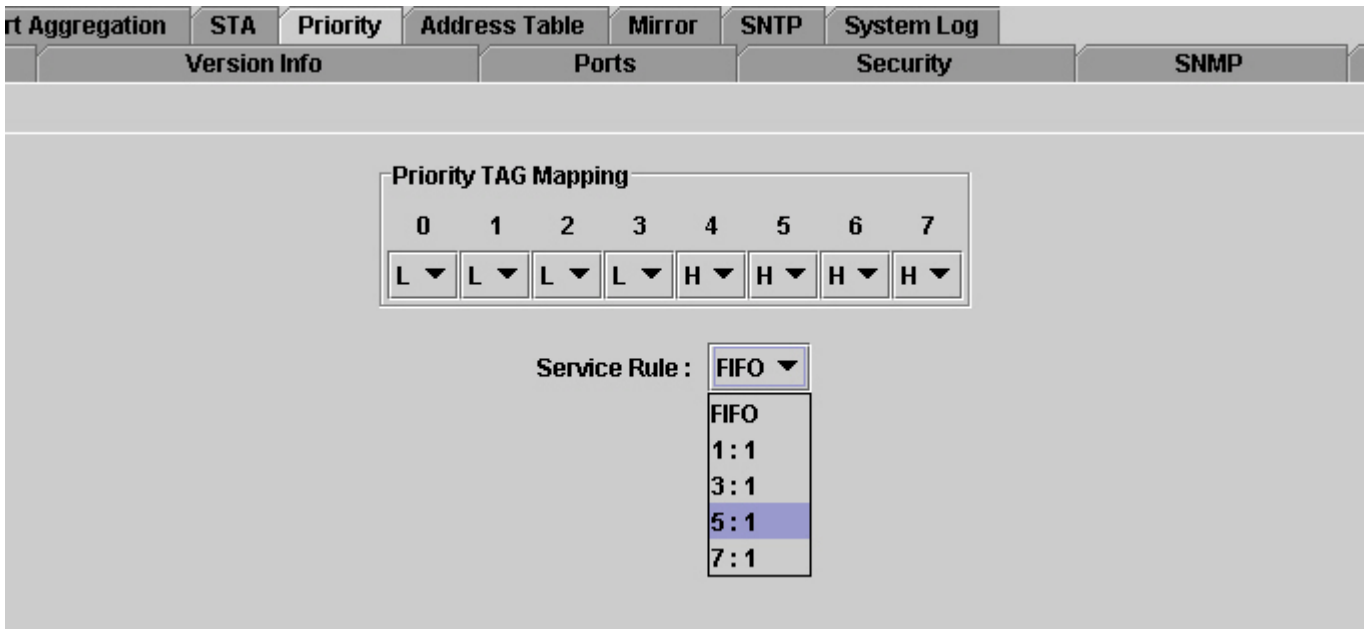
STA Port Configuration



Priority	The value of the priority field which is contained in the first (in network byte order) octet of the (2 octet long) Port ID
Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root, which include this port. 802.1D-1990 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
Fast Forward	The device omits from the 4 steps (Blocking – Listening – Learning – Forwarding) to 3 steps (Blocking – Listening – Forwarding) for speeding up specified port to be running when STA topology has been changed

3.12 Priority

This switch supports IEEE802.1p CoS with 2-level priority. There are 8 traffic classes and 5 Service Rules in the Priority Map. When one packet carries with priority-tag, which has specified a CoS (Class of Service) received by the switch, the specified CoS tag determines the priority (Low/High) level according to the Priority Map in the switch.



Service Rule:

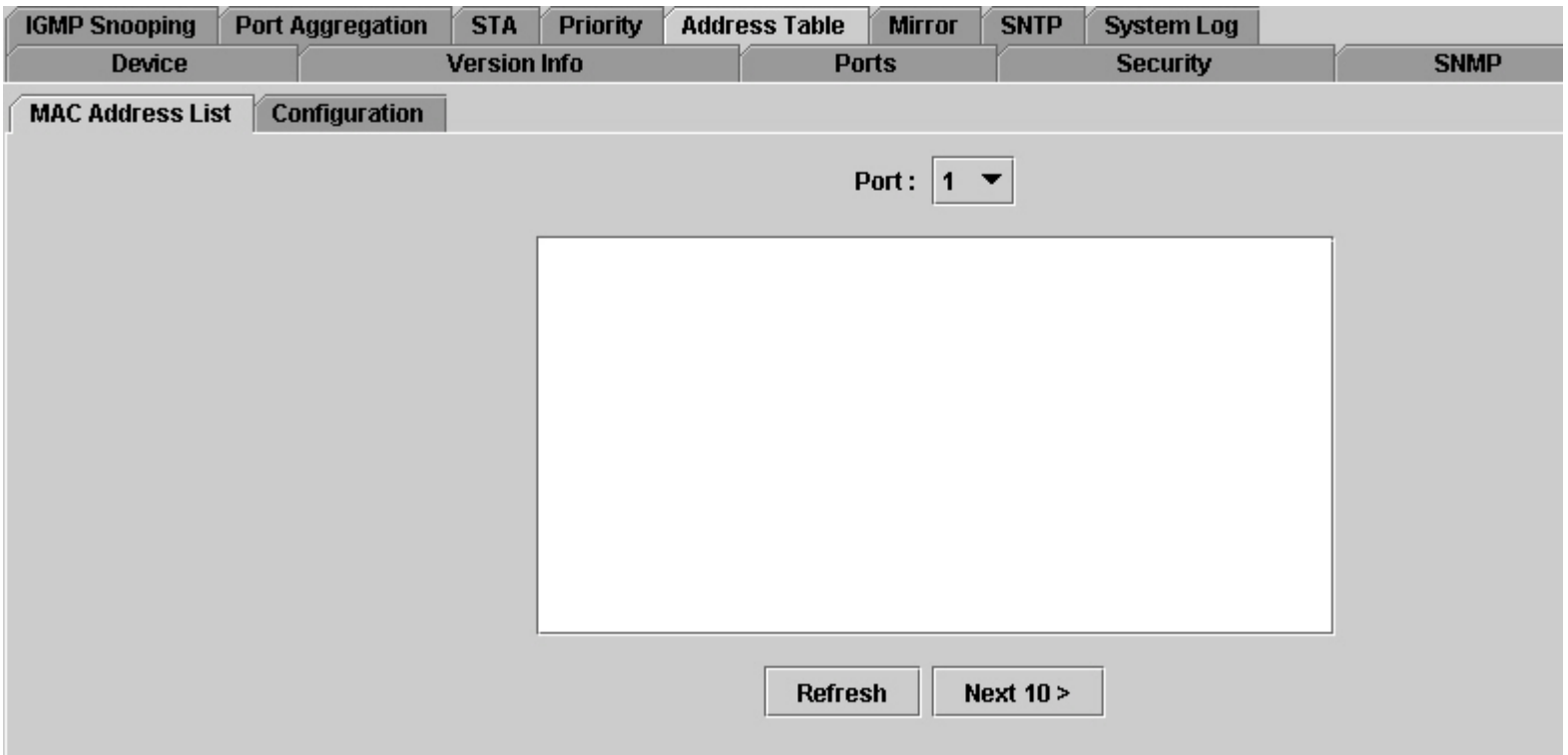
FIFO	The first in packet, the first out packet (No priority)
1:1	Send 1 high priority packet, then 1 low priority packet
3:1	Send 3 high priority packets, then 1 low priority packet
5:1	Send 5 high priority packets, then 1 low priority packet
7:1	Send 7 high priority packets, then 1 low priority packet

3.13 Address Table

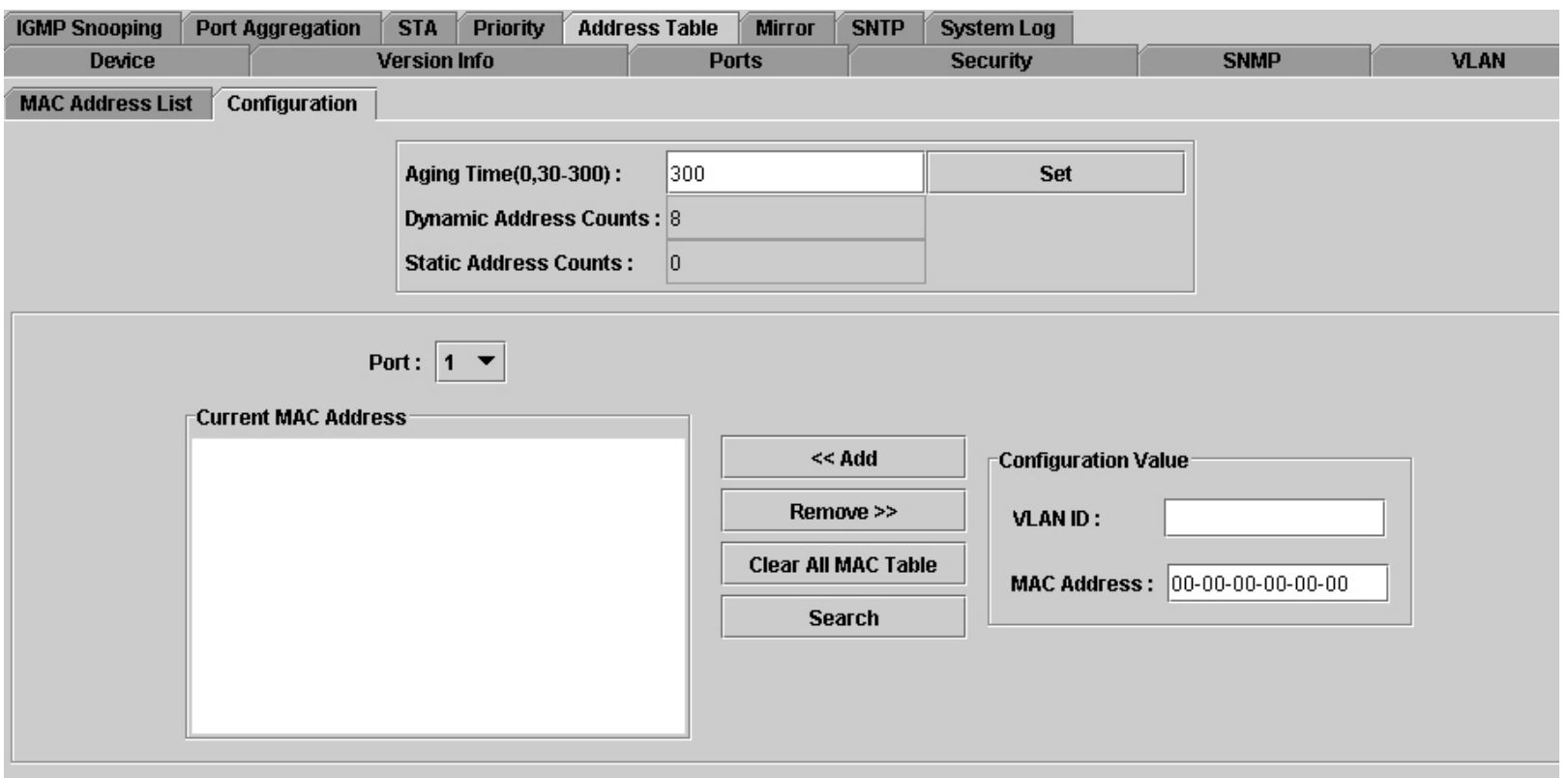
The address table is the learning table, which is composed of many entries and is the most important base to do packet filtering and forwarding.

MAC Address List

Choose the port you would like to view the address table and click the **Refresh** button, the MAC address table will be listed.



Configuration



Aging Time (0, 30-300 secs)	Set the period for keeping a accessing MAC address to be learned in the switch

	0: If the parameter is configured as “0”, the Aging Time is unlimited 30-300 secs: each number represents the time for a MAC to be learned
Dynamic Address Counts	Number of MAC addresses automatically learned by the switch
Static Address Counts	Number of MAC addresses manually added to the switch

To add a static address:

Click the combo box and select a port, then the MAC address table of the port appears.

Fill in configuration value (VLAN ID, MAC address), then click **<<Add** button (Note that ports on the switch are all defaulted to VLAN 1).

Note: The ports of Port Aggregation Group can not be added in Static Address table.

To remove a static address:

Click the static address in the MAC address table of the port.

Click **Remove>>** button to remove it from MAC address table.

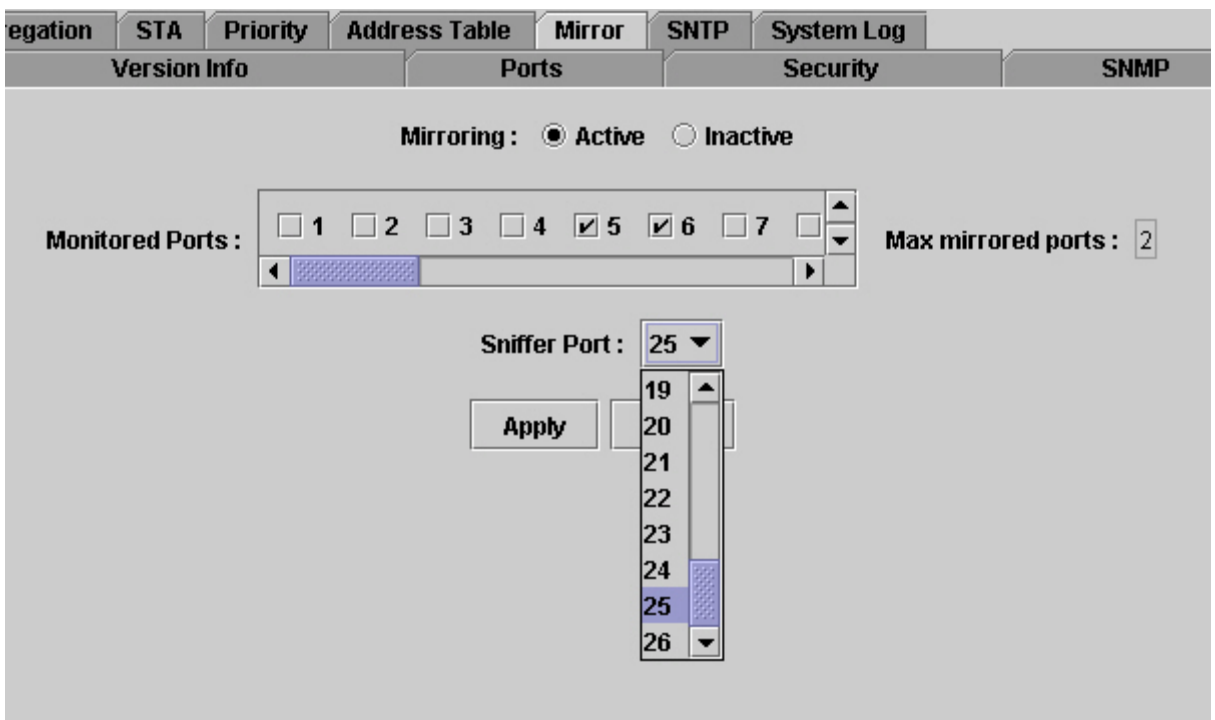
3.14 Mirror

Port mirror is used to mirror traffic from source port to a target port for analysis. Only 2 ports can be monitored (mirrored) simultaneously to 1 sniffer port (target port). (Note that the target port must be in the same VLAN as the source port)

Click “Active” radio button to activate port mirror.

Select ‘Monitored Ports’ (up to 2 ports).

Click ‘Sniffer Port’ combo box and select a sniffer port (target port) and click **Apply** to apply.



3.15 SNTP

This switch provides SNTP function. You can synchronize the time with the SNTP server on the Internet to ensure the correctness of system time.

To enable the function:

Select “Enable” in SNTP Function status.

To Add SNTP Server IP:

Enter the IP Address in the NEW textbox.

Click **<<Add** to add it on the list.

Click **Refresh** to get the latest Time.

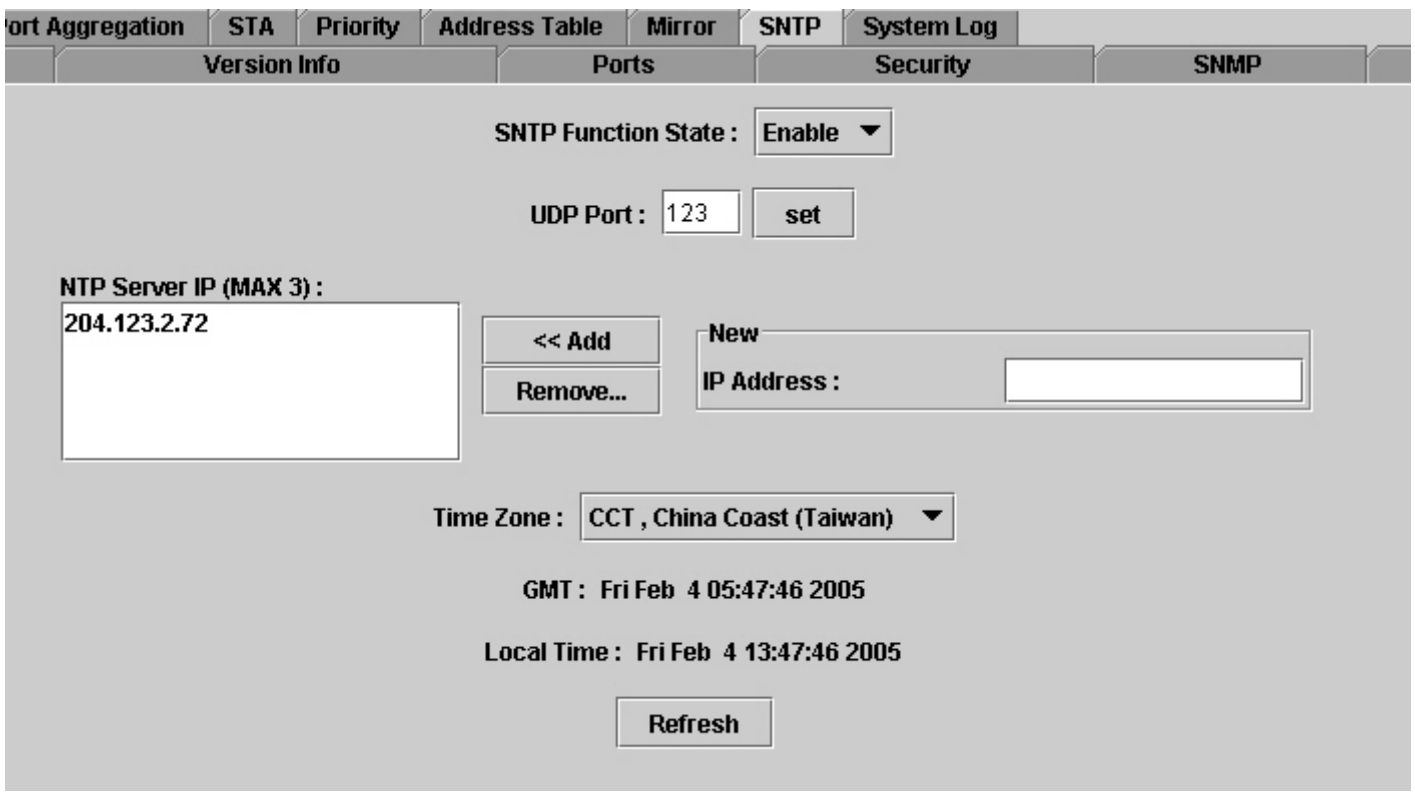
To Remove the IP:

Select the IP you want to remove.

Click **Remover…**

To select Time zone:

Select the Time Zone where the Switch is in the drop list.



3.16 System log

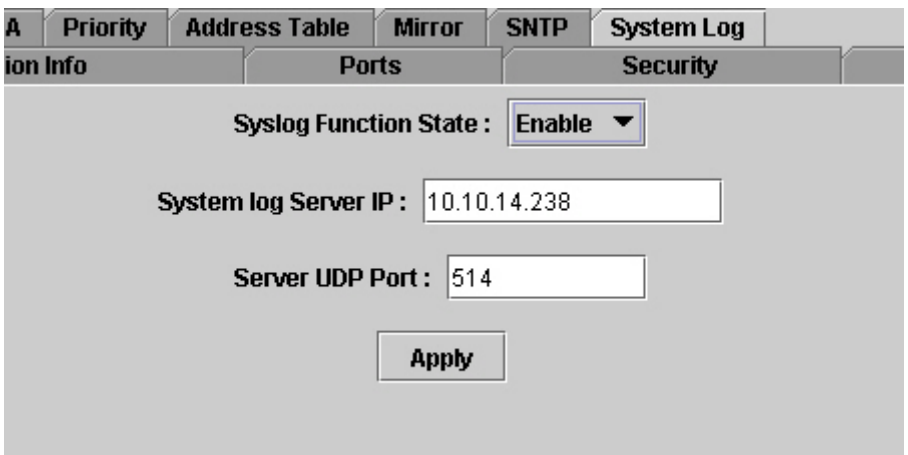
To sent the system log to remote server for backup,

Select “Enable”.

Enter the Server IP.

Enter the Server UDP port.

Click **Apply** to save.



4. Text-based User Interface

4.1 Setup the Connection

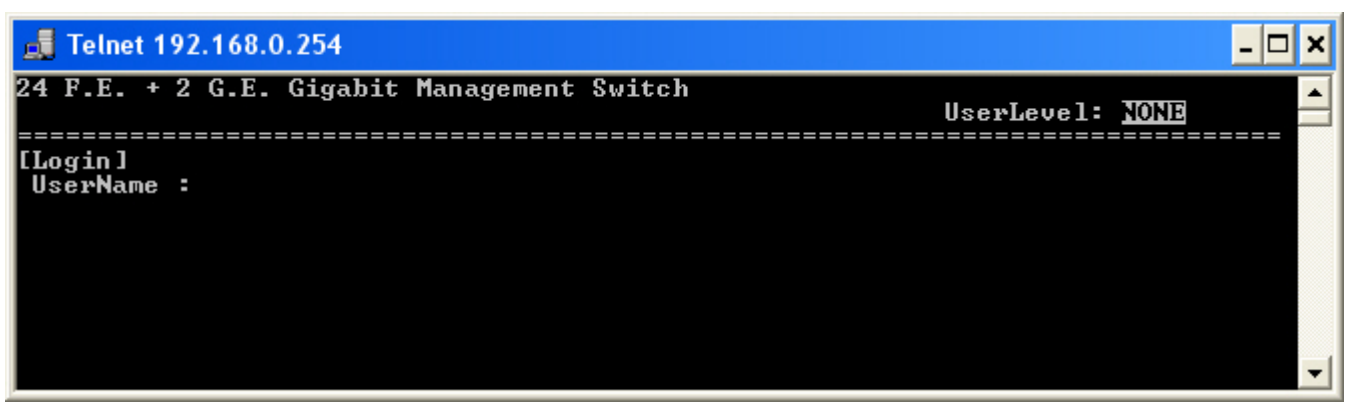
The switch provides other user interface to access by telnet and direct console. The management functions of Telnet program or console are exactly the same with web-based management interface but in text mode.

In-band Connection (Telnet)

To access the switch through a Telnet session, just start the Telnet program on a PC and connect to the switch. Factory Default value of system is:

IP Address:	10.10.0.1
Subnet Mask:	255.255.0.0
Default Gateway:	10.10.0.254

Press “Enter” key to begin login screen. Enter the username and password to login the system.



Login accounts:

- Username: ***admin*** Password: ***admin***
  “admin” can do any configuration except changing password.
- Username: ***guest*** Password: ***guest***
  “guest” can view the runtime information only.

Out-of-band Connection (Console)

To activate console port connection, attach a RS-232 cable (Straight-through) to the serial port of a PC running a terminal emulation program and configure the program as follows:

Baud rate:	**9600**
Parity:	**None**
Data bit:	**8**
Stop bit:	**1**
Flow control:	**None**

Press “Enter” key to begin login screen. Enter the username and password to login the management console. The management functions of console program are exactly the same with web-based management interface but in text mode.

Login accounts by default are:

- Username: ***root*** Password: ***superuser***
  “root” can do any configuration includes changing password and enable/disable management capability.

- Username: ***admin*** Password: ***admin***
  “admin” can do any configuration except changing password.
- Username: ***guest*** Password: ***guest***
  “guest” can view the runtime information only.

Note: Root is only for console access. Guest is not allowed accessing to web UI.

4.2 Main Menu

To get access to the CLI, you will have to get the username and password for login. Three default usernames/passwords are configured as root/superuser, admin/admin and guest/guest for different privilege levels. To Logout, you may press ESC in main manual.
(Note: We recommend users to configure a new username/password to prevent unauthorized users from accessing to the device.)
After success login, the main menu shows up and 6 sub-menus are listed:

[Main Menu]

1. ***System Information***
2. ***Management Setup***
3. ***Device Control***
4. ***User Authentication***
5. ***System Utility***
6. ***Save Runtime Configuration***

The CLI is constructed with menus and sub-menus. You can select a menu by inputting the number that corresponds to each sub-menu and press ESC to exit.

Commands are given by entering the command number listed on each menu. Select a number for your desire then press enter to configure.

EX, Select 1 then press enter to show the system information

[System Menu]

1. ***System Information***
2. ***System Configuration***

==========

<Press ESC key to go back previous screen>, or
Please input one value (1..2): 1 <enter>

4.3 System information

[System Menu]

1. ***System Information***
2. ***System Configuration***

System Information
Show system name, software version, system up time, device name, device location, management

capabilities.

System Configuration
Provide system contact, device name, and device location modification.

4.4 Management Setup

[Management Setup Menu]

1. ***Network Configuration***
2. ***Console Port Status Display***
3. ***SNMP Community Setup***
4. ***Trap Receiver Control***
5. ***Management Features Control***
6. ***Trap Filtering Setup***

Network Configuration
Provide IP address, Subnet Mask and Default Gateway modification. Please select 4 to apply changes after modification.

Console Port Status display
Display Console port status.

SNMP Community Setup
Provide new entry create, existing entry modification and deletion.

Trap Receiver Control
Provide new entry create, existing entry modification and deletion.

Management Features Control
For users to enable or disable the following capabilities:

1. Web-based Capability:
2. Telnet Capability:
3. SNMP Capability

Trap Filtering Setup
For users to enable or disable: Cold Start, Warm start, Link Up, Link Down, Test Only, Console Login, STA TCN and STA New Boot.

4.5 Device Control

[Device Control Menu]

1. ***Port Status/Configuration***
2. ***Address Table***
3. ***VLAN***
4. ***Security***

5. ***IGMP Snooping***
6. ***Mirror***
7. ***Statistic Information***
8. ***Priority Tag***
9. ***STA***
10. ***Port Aggregation***
11. ***SNTP***
12. ***System Log***

Port Status/Configuration

Show port status and provides port configuration.

Address Table

Provide the following configuration:

1. Display Address Table.
2. Mac Address Entry Created
3. Mac Address Entry Delete
4. Modify Aging Time
5. Search a Unicase Mac Address

VLAN

Provide the following configuration:

1. Select VLAN Mode: Tag based or Port based VLAN
2. Port Group VLAN: Status and Configuration

Security

You can add or delete Lock IP Entry after enable Lock IP function.

IGMP Snooping

For IGMP configuration or IP Multicast Registration Table checking.
(Note: Tag based VLAN mode should be selected first)

Mirror

For active/inactive Mirror function and further configuration.

Statistic Information

Enter port number for statistic information

Priority Tag

For priority tag mapping and service rule control

STA

The following configuration provided:

1. STA Status
2. STA Local Configuration
3. STA Port Status
4. STA Port Configuration

Port Aggregation

Show port aggregation status and configuration.

SNTP

The following configuration is provided:

1. SNTP Function
2. SNTP Server UDP Port and Time Zone Configuration
3. Add a New SNTP Server IP Entry
4. Delete an Old Existed SNTP IP Entry

System Log

For users to enable/disable System Log to make configuration.

4.6 User Authentication

Users are able to change the login username/password in this menu.

(Note: As default, only the username/password “root/superuser” is allowed to access this menu)

4.7 System Utility

[System Utility Menu]

1. ***System Restart***
2. ***Default Factory Reset***
3. ***Timeout Interval Setup***
4. ***TFTP Download***
5. ***Ping***
6. ***Search Location by Port Name***

System Restart

Commands are given to restart system

Default Factory Reset

Commands are given to reset to factory default.

Timeout Interval Setup

Set the time period for timeout.

TFTP Download

The menu includes the following configuration:

1. Modify Download Filename
2. Modify TFTP Server IP
3. Start TFTP Download

Ping

The menu includes the following configuration:

1. Modify Ping Count
2. Modify Ping Target IP

3. Start Ping

Search Location by Port Name

Provide users to search location by inputting port name.

4.8 Save Runtime Configuration

Provide users to save runtime configurations.

5. Specification

IEEE Standards		IEEE802.3, 10BASE-T IEEE802.3u, 100BASE-TX IEEE802.3ab, 1000BASE-T IEEE802.3z, 1000BASE-LX/SX IEEE802.3x, Flow control IEEE802.1q, Tag-based VLAN IEEE802.1p, Traffic prioritization (CoS) IEEE802.1d, Spanning Tree Protocol
Hardware & Performance	Processor SDRAM	8MB
	Processor Flash	2MB
	Packet Buffer	384KBytes
	MAC address table	6K entries
	10/100M, RJ-45	24
	10/100/1000M, RJ-45	2
	mini-GBIC slots	2 (share with Gigabit RJ-45 ports)
	Switching Fabric	8.8 Gbps
	Filtering/Forwarding Rate	10Mbps: 14,880pps/14,880pps 100Mbps: 148,800pps/148,800pps 1000Mbps: 1,488,000pps/1,488,000pps
	Switching Mechanism	Store and Forward
Key Features		Auto Negotiation Auto Uplink Flow Control for full duplex (IEEE802.3x) Port Trunking - 7 groups of port trunk - Max. 2000Mbps throughput one trunk Tag-based VLAN (IEEE802.1q) - Max. 255 VLAN groups Port-based VLAN - Max. 26 VLAN groups Spanning Tree Protocol (IEEE802.1d) Port Mirror IGMPv1 Snooping IP Lock to control access to system
Quality of Service		Class of Service (IEEE802.1p): - 2 priority queues per port - FIFO or Weighted Round-Robin Services Bandwidth Control

Management	Http/Web-based Interface Telnet/Command Menu interface Console/Command Menu interface Tftp/Firmware upgrade, Config Backup & Restore SNMPv1 System log
MIBs Supported	MIB II (RFC1213) Bridge MIB (RFC1493) Private enterprise MIB
Emission	FCC Class A, CE
Environment	Temperature: 0 to 40˚C (operating) Humidity: 10% - 90%, non-condensing (operating)
Dimension & Weight	441 × 130 × 44 mm, 1.62 kg
Power Supply	100-240V AC, 50-60Hz